Certification Authorities Software Team (CAST)

Position Paper
CAST-1

Guidance for Assessing the Software Aspects of Product Service History of Airborne Systems and Equipment

Completed June, 1998

NOTE: **This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Guidance for Assessing the Software Aspects of Product Service History of Airborne Systems and Equipment

Abstract:

This paper proposes an approach for assessing the software aspects of product service history of airborne systems and equipment. Service history is evaluated relative to four attributes of a system's product service history: the duration of the service period, the quality of the product and data accrued during the service period, the quality of the problem detection and reporting mechanism for the in-service system, and the quality of configuration control for modifications of the software during the service period. Guidance is offered on an approach for assessing the product service history data and for determining the amount of certification credit to allow based on the assessment of these attributes.

Key words:

Product service history, software, service period, assessment, certification credit

1. BACKGROUND

There are an increasing number of airborne systems whose functionality is provided by digital microprocessors and software. For analog systems, empirical data has been collected over the years that allows analysis and the determination of the reliability, maintenance and replacement of certified parts. Unfortunately, from the software perspective, these reliability numbers and replacement times do not apply. Software, unlike hardware devices and components does not break nor does it wear out. Also, hardware can and is usually tested thoroughly, even to the point of breaking, to ensure design flaws are not present. Software, because of increasing complexity and sophistication, cannot be assured to the same level and therefore cannot have a reliability number assigned it. A software design error may be present for years without manifesting itself or causing a failure condition that results in an unsafe condition for the aircraft or its occupants.

The recent focus of the certification authorities, aircraft manufacturers, and software system suppliers for "building quality into the software" and assuring it is to focus on the development and verification processes used by airborne system developers when building the software product. RTCA DO-178B / EUROCAE ED-12B is the latest guidance for assuring that a software product is produced to disciplined, best state-of-the-practice methods. This document is the primary means used by the aircraft certification authorities for assuring "safe" software.

This paper proposes using a similar process orientation for assessing the product service history of previously-certified software systems and how that assessment may be used to allow the certification applicant "credit" toward the certification of a new airborne system which uses the previously developed and certified software based on its pedigree and the processes in place during its service life on a previously certified system.

2. PURPOSE

RTCA DO-178B / EUROCAE ED-12B offers some guidance for assessing product service history. The purpose of this paper is to provide further clarification of the DO-178B concepts and some practical guidelines for assessing the product service history of airborne systems and equipment containing software on digital, programmable devices. It discusses some attributes to consider during assessment and using the assessment result, a means of determining the acceptability of product service history and the amount of credit to be granted.

Because the software under consideration is previously developed, the guidance of this paper should be tempered with the guidance of DO-178B for the use of previously developed software, Sections 12.1-12.1.6.

3. CERTIFICATION AUTHORITY SOFTWARE TEAM POSITION

The following represents one approach for assessing product service history for airborne systems and equipment containing software, but does not preclude the use of other means provided that the other means satisfy the criteria of RTCA DO-178B / EUROCAE ED-12B. It may be difficult or impossible to separate the software aspects of a system's product service history from the system aspects and hardware aspects. The hardware aspects of the system's product service history is not considered in this paper but may be considered by the certification authority in determining the acceptability of the applicant's approach and the data reported, for example, hardware qualification by similarity.

3.1 PRODUCT SERVICE HISTORY ATTRIBUTES

An assessment of RTCA DO-178B / EUROCAE ED-12B Section 12.3.5 allows the required criteria for product service history to be viewed in six categories as illustrated in Table 3.1-1.

CATEGORY	**DO-178B REFERENCES**
MEANS OF COMPLIANCE	**11.1g., 12.3.5j.**
SERVICE HISTORY DURATION	**12.3.5j.(2)**
PRODUCT QUALITY	**12.3.5d., e., g., j.(1)**
PROBLEM DETECTION/REPORTING	**12.3.5b., h., i., j.(3), j.(4), k.**
MODIFICATIONS AND CONTROL	**12.3.5a., c., f.**
EVIDENCE OF COMPLIANCE	**11.20g.**

Table 3.1-1 – DO-178B Service History Categories

For the first category, means of compliance, the guidance of RTCA DO-178B / EUROCAE ED-12B appears straightforward, that is, the applicant should define their plans and processes for complying with the product service history guidance of Section 12.3.5 in the Plan for Software Aspects of Certification. Likewise for the last category of the table, evidence of compliance, the guidance of RTCA DO-178B / EUROCAE ED-12B appears straightforward, that is, the applicant should summarize how the product service history data provided and additional activities conducted have satisfied the criteria for gaining credit for product service history. It is the other categories that this paper provides additional guidance for determining the acceptability of an applicant's request for claiming product service history credit.

3.1.1 PRODUCT SERVICE HISTORY DURATION

The duration of the service period is an important attribute for determining the amount of credit to be granted. If a airborne system has software that has functioned full-time in all flight phases during "normal operation" with no changes and no problems detected or reported, and the applicant is proposing to install it in a very similar or identical operational environment, the certification authority may allow a great deal of product service history credit.

DO-178B REFERENCES Related to Product Service History (PSH) Duration: 12.3.5.j.(2), 12.1.4.e.

The certification engineer may want to consider the following list of questions when assessing the duration of the product service history (service period):

- How were the in-service operational hours of the product measured?
- How reliable is the means of measuring in-service operational hours?
- Is the service history duration acceptable for considering granting credit? And how much credit can be allowed based on the duration?
- How are the in-service operational hours of the product reported?
- How reliable is the means of reporting in-service operational hours?
- Are all of the software functions and components within the system utilized for normal operations (i.e., no dead code, no deactivated code, no unused components, etc.)?[12.3.5.g.]
- If not, what parts (or percentage) are used for normal operation and what parts (percentage) aren't?
- What is acceptable versus unacceptable duration for portions of software unused during normal operations relative to PSH credit? For example, can any credit be allowed for software components that were not active or used during the service period?
- How relevant is the software level(s) of the system in determining the acceptability of PSH duration?

- What conclusions, assurance and/or confidence about the software product can be justified from the service history duration and supporting data?

3.1.2 PRODUCT QUALITY

The quality of the software in the system should be considered for determining the amount of credit to be granted. For example, if the system has been in service for an acceptable duration and its software has not changed nor had any problems reported with it, the software develops a "pedigree" that should be considered, especially if the new operational environment is identical or very similar to its previous environment. Of course, this assumes that data exists that demonstrates the stability and maturity of the software. The collection of this supporting data may be done through a number of means. For example, the certification authorities has visibility to certain types of data (FAR 21.3 reported data, airworthiness directives, etc.). The applicant has visibility to more detailed data including in-service problem reports, system failures, part number revisions, modifications, laboratory test results, etc.. And the manufacturer of the system normally has access to the most detailed data, including acceptance test results, analyses of failed units, software problem reports, problem report history, problem analyses, software version control data, software component-level test results, etc.. The applicant is responsible for the collection of data to support the software pedigree and for justifying the requested certification credit based on the software's pedigree.

Of course, this may be a very difficult task if any of the following are true:

- the service period duration is short,
- the new operational environment is very dissimilar,
- product quality data is unavailable, and/or
- the product is not stable nor mature (e.g. many problem reports and/or modifications occurred during the service period).

DO-178B References Related to Product Quality:
12.3.5.j.(2), 12.1.2c., 12.1.4.a., c., d., 12.1.6

The certification engineer may want to consider the following list of questions when assessing the quality of the product and its data:

- How much credit can be given for software that was developed to previous software standards (RTCA/DO-178, DO-178A, MIL-STD 1679, MIL-STD 2167, etc.)? Or to no standards?
- How much credit can be given for very old, poorly documented software products?
- What is the similarity between the previous operational environment and the new operational environment? [12.3.5.e., f., j.(1)] What are the significant differences?
- How similar is the usage of software components between the previous product and the new product? [12.3.5.d.] What are the significant differences?

- What is acceptable versus unacceptable significance (impact) of errors detected and reported?
- What is an acceptable versus unacceptable total number of errors detected and reported?
- What is acceptable versus unacceptable number of modifications during the service period?
- What is acceptable versus unacceptable for the significance or impact of the modifications during the service period?
- What is the relevance of the software level(s) of the software components for consideration of acceptable versus unacceptable error rates or modifications?
- Can a reliability number be assigned to the system (and inherently to the software intrinsic to the system's operation) because of acceptable PSH (e.g., 1 million operational hours with no errors detected or reported and no modifications)?
- What data, evidence and assurance should be required of the applicant for the requested PSH credit?
- What conclusions, assurance or confidence about the software product can be justified from the product quality data?

3.1.3 PRODUCT SERVICE HISTORY ERROR DETECTION AND REPORTING

There are three aspects relative to error detection and reporting of the product during the service period: the means of collecting error data, the integrity of the data collected, and the significance or impact of the error data on the product. The number and significance of errors collected about a product establishes an important aspect of the software product's quality. For example, if a very good means of collecting quality error data is established and analysis of the collected error data indicates no or few software-related errors were detected and none of significance, this may indicate that the software is robust and of good quality, especially contrasted with software that has a history of problems, many modifications and/or multiple, significant software-related failures. There are various means of collecting in-service problem report data, for example, maintenance download of built-in test equipment (BITE) fault information, shop BITE download of failed units and analyses of their causes, etc.. Here again, the airlines, applicant and software system supplier will have increasingly detailed data regarding the problem reports associated with a system and its software and the resolution of those problems. The applicant is responsible for determining the error detection and reporting means during the service period, for analyzing the significance of reported problems, and for justifying any credit claimed based on this aspect of the software product's quality.

In assessing detected and reported errors toward assessment of the software, it is important that the applicant and/or supplier has the capability to determine and distinguish between these different types of failures and errors:

NOTE: **This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

a. software errors,

b. hardware failures,

c. system enhancements (functions, features and capabilities not intended to be addressed by the system, i.e., product improvements).

Obviously, only the software error type should be considered for determining the software quality. Of course, the significance and airplane-level and system-level impacts of the errors and failures should also be considered. For example, a software error that has a safety impact is more significant than a error that has a crew workload impact, which in turn, is more significant than error resulting in a nuisance or error which is not even apparent to the flight crew.

DO-178B PSH Error Detection and Reporting Related References:
12.3.5.b., j.(3), j.(4), h., i., k., 12.1, 12.1.5.b.

The certification engineer may want to consider the following list of questions when assessing the error detection and reporting of the product during its service period:

- What were the means of detecting in-service errors? How reliable is the means of error detection? Are all errors detected?
- What counts as an error? (and what doesn't?)
- What are the means of recording in-service errors? How reliable is the means of error recording? Are all detected errors recorded?
- What are the means of reporting in-service errors? How reliable is the means of reporting errors? Are all detected and recorded errors reported?
- How are reported errors categorized to determine their significance and impact? Are software-related errors categorized separately from system or hardware reported errors?
- Are non-service errors relevant (e.g., errors detected during lab testing)?
- Are product improvements or unresolved, unincorporated software problem reports relevant with regard to PSH credit? [12.3.5.a.]
- What conclusions, assurance or confidence about the software product can be justified from the error detection, reporting and resolution?

3.1.4 PRODUCT MODIFICATIONS AND CONFIGURATION CONTROL

Configuration control of the system and software components and of modifications to the software and its environment are essential for determining credit based on product service history. In other words, if the software and modifications to it haven't been controlled, the software has no pedigree and is of very questionable quality. Unless the applicant can demonstrate that the system and software have been controlled throughout the service period, there should be no further discussion of granting credit and the applicant should be required to comply fully with the objectives of DO-178B.

The applicant and/or the software supplier should have detailed records of the original product's configuration as well as records for each modification made to the original certified part and supporting data which confirms the acceptability of each modification. Usually, the configuration is defined in a system configuration index document (or equivalent), a unit configuration index document, and/or a software configuration index (or version description document or equivalent).

For software modifications, the configuration is usually re-established in a new configuration index and the modification process is summarized in the software accomplishment summary. This forms the basis for software aspects of the certification of the modified system.

DO-178B References Related to PSH Configuration Control and Modifications: 12.3.5.a., c., f., h., 12.1.1a.-e., 12.1.2, 12.1.5

The certification engineer may want to consider the following list of questions when assessing the configuration control and modification of the product during its service period:

- Is there acceptable evidence that all components of the system and software have been change controlled throughout the service period? How reliable is this evidence?
- Have all changes to the system and software been documented and complied with appropriate procedures throughout the service period? Is there evidence of this and how reliable is the evidence?
- Has the applicant/supplier maintained a history and rationale for all modifications to the system and software throughout the service period?
- Was the modification process defined, is it acceptable and was it adhered to for all modifications to the system? Is evidence of this available and is it reliable?
- For each software modification, was a change impact analysis conducted and the results of that analysis used to determine the scope and level of regression testing relative to the software level? Are analysis and test results available?
- Were the results of each software modification of the system summarized in an accomplishment summary which was approved by the certification authority?
- Are the number and significance of the modifications such that it is acceptable to allow PSH credit?
- How is the validity of modified system and/or software for PSH credit established?
- What conclusions, assurance or confidence about the system and/or software can be justified from the configuration control and modification data?

3.2 GUIDANCE FOR ASSESSING PRODUCT SERVICE HISTORY ATTRIBUTES

From the preceding sections, it is obvious that there are many factors to consider when determining how much credit can be granted for the product service history of a system and its software. The above sections are not a complete treatise of the potential issues or questions, but are intended to prompt discussion which will aid in identifying other issues and questions.

This section attempts to address the question: After the certification engineer has determined the answers to the relevant questions and reviewed the applicant-supplied data, how does the engineer determine if credit should be allowed, how much credit should be allowed, and what additional activities or assurances are needed to approve certification of the subject airborne system?

What conclusions, assurance or confidence about the software product can be justified from the product service history attributes (duration, product quality, error detection and reporting, configuration control and modifications)?

Taking into account the product service history attributes, individually and collectively, how much credit can be allowed for the current certification effort?

Is the software level(s) of the product a factor for determining the relevance of the product service history and the amount of credit to be granted?

3.3 GUIDANCE FOR DETERMINING PRODUCT SERVICE HISTORY ACCEPTABILITY AND CREDIT

Table 3.3-1 below lists some of the product service history attributes relative to acceptability versus the unacceptability of the data for allowing certification credit based on service history:

TABLE 3.3-1 – Product Service History Attributes Acceptability

Product Service History Attribute	Not Acceptable	<--------------	----------------	--------------->	Acceptable
Service Duration Length	**Short**	<--------->	Moderate	<--------->	Long
Change Control During Service	**None**	<--------->	Marginal	<--------->	Total
Proposed Use Versus Service Use	**Different**	<--------->	Similar	<--------->	Identical
Proposed Environment to Service Environment	**Different**	<--------->	Similar	<--------->	Identical
Number of Significant Mods During Service	**Many**	<--------->	Few	<--------->	None
Number of Software Mods During Service	**Many**	<--------->	Few	<--------->	None
Number of Hardware Mods During Service	**Many**	<--------->	Few	<--------->	None
Error Detection Capability	**None**	<--------->	Some	<--------->	All
Error Reporting Capability	**None**	<--------->	Some	<--------->	All
Number of In-Service Errors	**Many**	<--------->	Some	<--------->	None
Amount/Quality of Service History Data Available and Reviewed	**None/ Low**	<--------->	Some/ OK	<--------->	Much/ High

LEGEND:	**No Credit Allowed**	Little if any Credit Allowed	Engr. Judgment for No or Some Credit Allowed	Credit allowed based on Engr Judgment	Credit Allowed

As one can see from Table 3.3-1, engineering judgment by the certification engineer must be used for determining the acceptability of product service history. The engineer must also assess the subjective terms used, such as, “some” and “few” to determine if credit is to be allowed and how much. The attributes listed are only offered as guidance, there may be other attributes the engineer may want to considered as well, for example, the reputation of and the engineer’s experience with the product service history applicant.

Also, the product service history attributes assessment will probably not fall readily into a single column of the table where the determination of the acceptability of the service history can be easily determined. The engineer will also need to use judgment in determining the “weight” of various attributes’ for determining acceptability. The engineer should consider, however, that the attributes are related and none can stand entirely alone for assessing acceptability. For example, if a product has a long service history duration but was not under configuration control, then it has no pedigree and duration alone would not be an acceptable attribute to allow much credit.

NOTE: **This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Table 3.3-2 attempts to relate the acceptability of the product service history data of Table 3.3-1 to the software level(s) of the software components of the airborne system or equipment being assessed in terms of its relative importance. Obviously, for the higher software levels (e.g., RTCA/DO-178B Levels A and B, DO-178A Level 1), the assessment criteria should be much more stringent than those for the lower software levels (e.g., D, E and 3).

TABLE 3.3-2

Product Service History Attribute	SwL A/1	SwL B/1	SwL C/2	SwL D/3	SwL E/3
Acceptable Service Period Duration	*	*	*	x	
Acceptable Change Control During Service	*	*	*	x	x
Similar/Identical Proposed Use to Service Use	*	*	*	x	x
Similar/Identical Environment to Service Environment	*	*	*	x	x
Acceptably Low Number of Significant Mods During Service Period	*	*	*	x	
Acceptably Low Number of Software Mods During Service Period	*	*	x	x	
Acceptably Low Number of Hardware Mods During Service Period	*	*	x	x	
High Quality of Error Detection Capability	*	*	*	x	
High Quality of Error Reporting Capability	*	*	*	x	
Acceptably Low Number of In-service Errors	*	*	x	x	
Acceptable Amount and Quality of Service History Data Available and Reviewed	*	*	x	x	

LEGEND:	SwL = Software Level DO-178B/A	* = Very Important	x = Important	Blank = Less Important	

4. CONCLUSION

The previous sections have attempted to identify some of the issues confronting the certification authority engineer when trying to assess the software aspects of the product service history of airborne systems and equipment, and to suggest an approach for evaluating the service history data and determining the amount of certification credit to be granted based on that assessment. If little or product service history data is available which addresses these attributes of the product, the engineer should allow little or no credit and will need to determine other types of assurance the applicant must provide to allow for certification of the new system (for example, review of existing product data, additional laboratory, ground or flight testing, etc.). This will also be the case if product service history data is available but of questionable quality.

***NOTE:* This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

In summary, the certification engineer could use of following approach for determining the validity of an applicant's claim for product service history for previously developed software to be used in a new airborne system application:

1. Identify for the applicant the type and detail of data needed for their claim.
2. After receiving the data, determine that sufficient data has been made available to assess the applicant's claim. If more data or more detailed data is needed, request it from the applicant.
3. Using the guidance from Table 3.3-1, determine the acceptability of the product service history data relevant to the product service history data attributes listed and other applicable criteria.
4. Using the guidance of Table 3.3-2, determine the importance of the product service history data attributes relative to the software level of the application.
5. If, in the engineer's judgment, the data is acceptable for the software level(s) of the system, determine the amount of certification credit to be granted and inform the applicant of any other assurances that are needed, if any, for certification of the new system.
6. If, in the engineer's judgment, the data is unacceptable, inform the applicant and propose other means of gaining assurance of the acceptability of the system for certification.
7. Document the process used for assessing the product service history and identify any improvements to the process or additional criteria to consider for future assessments.

***NOTE:* This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**